RSA® Archer eGRC

SENSITIVE BUT UNCLASSIFIED

(b) (7)(E)

SOC Incident Management System

IMS User Contact:	(b) (7)(E)	**Restrict Access To:**	(b) (7)(E)
Record Permissions Group:		**Record Source:**	

Contact Details

Enter the NASA AUID or email address of the Contact, and click "Lookup Contact Details" to automatically retrieve the information.

AUID:		**Email:**	

Enter Contact information below if the primary contact is not an IMS user

Contact Last Name:	(b) (7)(E)	**Contact First Name:**	(b) (7)(E)
Contact Role:		**Contact Office Phone:**	
Contact E-mail:		**Contact Cell Phone:**	
Contact AUID:		**Contact NASA Center:**	
Contact Building:		**Contact Room Number:**	
Contact Type:			

General Details

SOC Tracking Number:	(b) (7)(E)	**Categorization:**	(b) (7)(E)
Date Record Created (UTC):		**Incident Time Zone:**	
Title:			

Brief Description:	(b) (7)(E) Title: Mystery group hacks US military, Harvard, NASA, more Author: Emil Protalinski Source: ZDNet Date Published: 2nd May 2012 Excerpt: '....A hacker group calling itself "The Unknowns" claims to have hacked 10 organizations around the world, gaining administrator access for all and leaking data for some. Most are related to the U.S. government or another international legislative body, while the rest just seemed like random targets. The Unknowns listed 10 victim websites for which it publicly posted administrator accounts and passwords: NASA - Glenn Research Center U.S. military U.S. Air Force European Space Agency Thai Royal Navy Harvard University Renault French ministry of Defense Bahrain Ministry of Defense Jordanian Yellow Pages In addition to revealing how to access the computer systems of the organizations in question, The Unknowns also posted screenshots showing they gained accessed to each and every one. More importantly, the group put together military documents from their hacks, and uploaded the collection to MediaFire: Part 1 (177.79MB) and Part 2 (37.37 MB)......' To read the complete article see: http://www.zdnet.com/blog/security/mystery-group-hacks-us-military-harvard-nasa-more/11789 (b) (7)(E) (b) (7)(E)

Current Status:	(b) (7)(E)	**Assigned To:**	(b) (7)(E)
Current Priority:		**Also Notify:**	
CUI:		**Notify on Save:**	
Ok To Close:			

US CERT Reporting

Risk Rating:			
Information Impact:		**Functional Impact:**	
Recoverability:		**Attack Vectors:**	
Critical Service or System:		**Classified Incident:**	
Major Incident:		**High Value Assets (HVA):**	
Reportable to Congress:			
Observed Activity:		**Number of Records Impacted:**	
Location of Observed Activity:		**Number of Systems Impacted:**	
Actor Characterization:		**Number of Users Impacted:**	
Action Taken to Recover:		**Number of Files Impacted:**	

The fields below hold the US-CERT Reporting fields that were in force from October 1, 2015 through March 31, 2017. The are included here for reporting purposes only.

Functional Impact old:		**Informational Impacts old:**	

		Recoverability Impact old:	

Related Tasks

Task ID	Assigned To	Due Date (UTC)	Priority	Status	Description	Resolution
No Records Found						

Related Incidents

Select Relationship:		Relationship Description:	

Parent Incident

SOC Tracking Number	Current Status	Title
No Records Found		

Child Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Sibling Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Incident Details

Time Incident Started:		Time Incident Started (UTC):	
Time Incident Detected:		Time Incident Detected (UTC):	(b) (7)(E)
Center Affected by Incident:	Other	Overall Impact (reference):	
US-CERT Category:	(b) (7)(E)	Incident Subcategory:	
US-CERT Tracking Number:		ESD Ticket #:	
Resolution Status:		Malware Family:	
		Highest level of access gained:	
Primary Method used to Identify Incident:	(b) (7)(E)		
Primary Attack Category:			

Primary Vulnerability Type:		**Lost or Stolen NASA Equipment:**	

Lost or Stolen NASA Equipment Application

Tracking ID	Cause of Loss	Type of System Lost	Description of Circumstances
No Records Found			

Host Information

NASA Hosts

IP Address	IPv6 Address	Host Name	Center/Facility
No Records Found			

External Hosts

IP Address	External IPv6 Address	Host Name	Position in this attack
No Records Found			

Campaigns

Campaign Name:		**Reviewed By TVA:**	
Campaign Comment:		**Confirmed By TVA:**	
		Is APT:	

Indicators of Compromise

(b) (7)(E)

(b) (7)(E)

IOC Detection

Name	Type	Comment
No Records Found		

Root Cause Statement

The Root Cause Statement can be constructed from the following fields like so:
"SOURCES source realized CATEGORIES using METHODS exploiting CAUSES (with additional FACTORS) gaining OBJECTVES."
See the help for the individual fields for more information about what the various values mean and their context.

Root Cause Sources:		**Root Cause Categories:**	
Root Cause Methods:		**Root Cause Causes:**	
Root Cause Factors:		**Root Cause Objectives:**	

Reporting Organizations

Reporting Date (UTC)	Reporting Local Date	Reporting Local Time Zone	Reporting Notes	Reporting Number	Reporting Organization	Reporting Organization Contact
No Records Found						

Impact of Incident

NASA Programs, Projects, and/or Operations:		**People:**	
Data (at Rest or Transmission):		**System:**	
Cost:		**Sophistication / Nature of Attack:**	
Number of systems affected by this incident:		**Number of NASA Centers/ Facilities affected by this incident:**	
Number of accounts affected by this incident:		**Critical Infrastructure Impacted:**	
Other Impacts:			
Overall Impact:	(b) (7)(E)		

Containment Actions

Incident Containment System Action:	
Incident Containment Network Action:	

Recovery Actions

Incident Recovery System Action:	
Incident Recovery User Action:	

Recommendations

Root Cause:	
Lessons Learned:	

Costs

Center (Hours):	(b) (7)(E)	**Center (Dollars):**	(b) (7)(E)
NASA SOC (Hours):		**NASA SOC (Dollars):**	
NASA NOC (Hours):		**NASA NOC (Dollars):**	
Other Costs (Hours):		**Other Costs (Dollars):**	

Total Costs in Hours and Dollars are automatically calculated as the sum of the individual costs above. Center IR teams or managers should enter the Center costs, the NASA SOC Manager should enter the SOC Costs and the NOC Manager should enter the NOC costs, if any, in order to arrive at the Total Cost.

Total Cost (Hours):	(b) (7)(E)	**Total Cost (Dollars):**	(b) (7)(E)
Description of Costs:			
System Down Time (Days):		**System Down Time (Hours):**	

Timeline

Date Record Opened (UTC):	(b) (7)(E)	**Date Record Confirmed**	(b) (7)(E)

	(b) (7)(E)	(UTC):	(b) (7)(E)
Date Record Contained (UTC):		Date Record Resolved (UTC):	
Date Record Closed (UTC):			
Time in Open:			
Time in Confirmed:		Time to Confirm:	0.00
Time in Contained:		Time to Contain:	0.03
Time in Resolved:		Time to Resolve:	0.03
Time in Closed:		Time to Close:	0.10
Number of Days to Resolve:			

Journal Entries

Entry	Entry Date	IMS User
(b) (7)(E)		

(b) (7)(E)

Email Attachment :

Attachment(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

History Log

View History Log